A Phishing attack is generally characterized by a lure, hook, and catch

The Hook

The hook is a malicious website designed to look and feel like a legitimate website. The authentic-looking website asks the victim to disclose privacy-related information, such as user identification and password. Often the hook is an obfuscated URL that is very close to one the victim finds legitimate and is really a site under the attacker's control.

The Lure

The lure is an enticement delivered through email. The email contains a message encouraging the recipient to follow an included hypertext link. The hyperlink often masks a spoofed uniform resource locator (URL) of a legitimate website.

The Catch

The catch is when the originator of the phishing message uses the information collected from the hook to masquerade as the victim and conduct illegal financial transactions.

UNCLASSIFIED

Today, more than ever, spear phishing attacks are focusing on national security targets and our federal users. For this reason, it is important to understand how to identify a phishing email and what steps to take to prevent identity theft, unauthorized system access, or mission compromise.

Remember to…

STOP, THINK,** before you **CLICK!

Don't Be Phished!

ONE click could compromise. . .

- your personal information
- your agency's information
- your computer system
- your computer information

Don't Be Whaled!

"Phishing the Big Fish"

As Senior Leaders, you are in the spotlight of your agency. This makes you a more valuable target for nefarious people on the Internet.

For Phishing training visit:
http://iase.disa.mil/eta/phishing/Phishing/

UNCLASSIFIED

UNCLASSIFIED

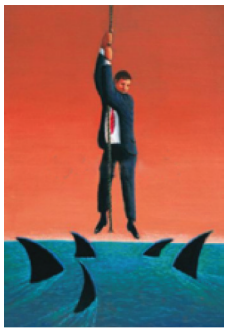
Phishing Warfare

Executive Handout

UNCLASSIFIED

Phishing is largely a criminal activity employing social-engineering tactics to defraud Internet users of sensitive information and steal credentials, money and/or identities. A phishing attack begins with a spoofed email masquerading as trustworthy electronic correspondence that contains hijacked brand names of banks, credit card companies, or ecommerce sites. The language of a phishing email is misleading and persuasive by generating either fear or excitement to ultimately lure the recipient to a fraudulent Web site.

Spear Phishing is an e-mail spoofing fraud attempt that targets a specific organizations and users, seeking unauthor - ized access to confidential data. Spear phishing attempts are not typically initiated by "random hackers" but are more likely to be conducted by organized perpetrators out for financial gain, trade secrets, or national security information. As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source.



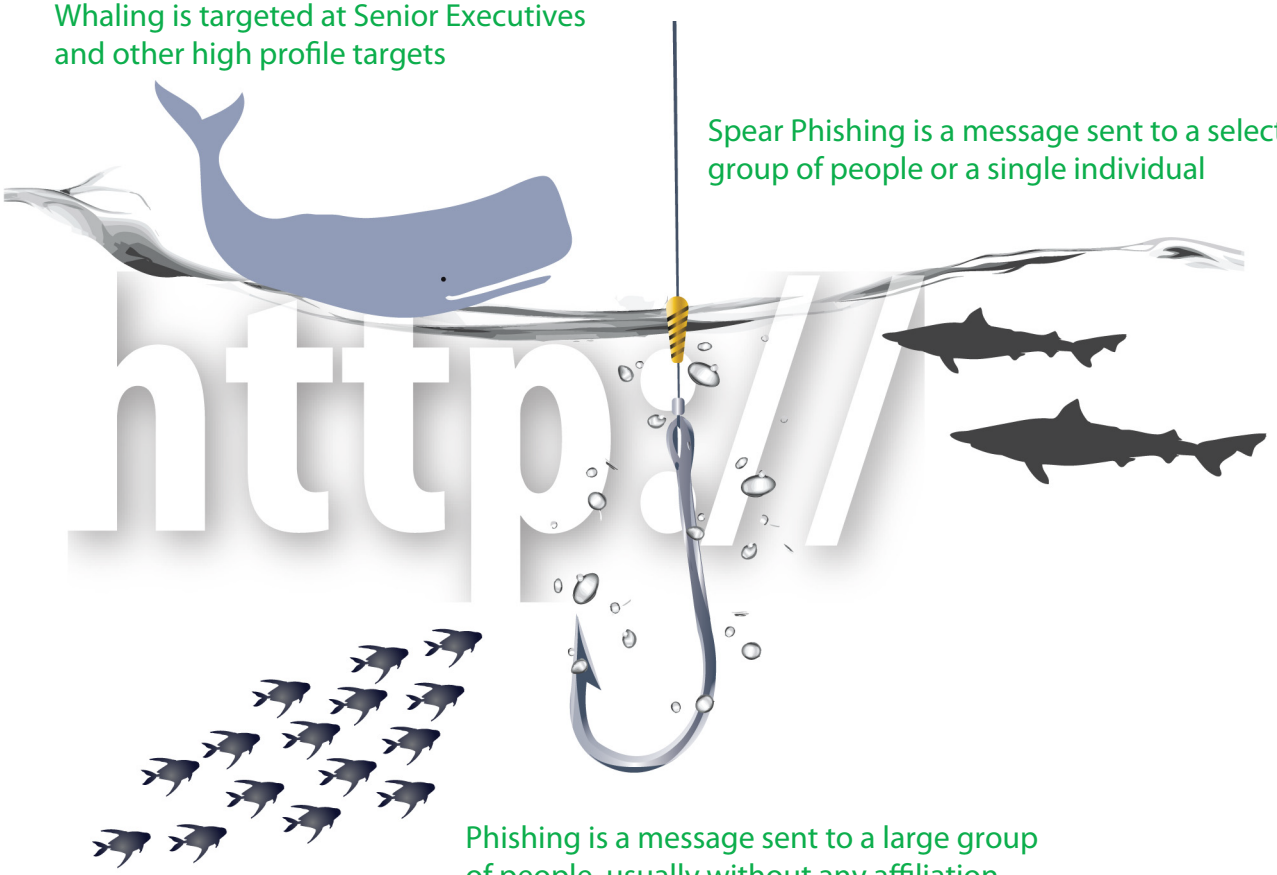
Whaling is a spear phishing attempt to target Senior Executives/Leadership (i.e. the big fish).

UNCLASSIFIED

UNCLASSIFIED

Whaling is targeted at Senior Executives and other high profile targets

Spear Phishing is a message sent to a select group of people or a single individual



Phishing is a message sent to a large group of people, usually without any affiliation

What could be the Technical and Operational Impact?

In 2010, during a joint military exercise sponsored by a functional Combatant Command, a service Red Team (as part of their exercise pre-positioning phase), identified 190 potential targets (first name, last name, and military ranks). The Red Team deduced, selected, and targeted 7 user e-mail accounts with 1 phishing email. The phishing e-mail was neither digitally signed nor encrypted and contained malicious code attached to a Microsoft Excel file. 2 of 7 targeted users clicked the phishing email.

This set forth a spiral of events that allowed the Red Team to establish connections, steal files, capture data, and remotely execute commands of their choosing. The Red Team eventually achieved Domain Admin Privileges over more than 6,800 user accounts, 5,400 computer accounts, and all associated password hashes. The detrimental impact on the technical and operational capabilities of the organization to perform its mission was high (high impact to the confidentiality and integrity of information systems and networks).

UNCLASSIFIED

UNCLASSIFIED